Uɴɪᴛᴇᴅ Sᴛᴀᴛᴇs Pᴀᴛᴇɴᴛ ᴀɴᴅ Tʀᴀᴅᴇᴍᴀʀᴋ Oꜰꜰɪᴄᴇ

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/822,548	03/30/2001	Matthew D. Wood	42390P10451	7654

7590 09/21/2005	**EXAMINER**
Michael A. DeSanctis	PYZOCHA, MICHAEL J
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP	

ART UNIT	PAPER NUMBER
2137	

Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

DATE MAILED: 09/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/822,548	WOOD ET AL.
	Examiner	**Art Unit**	
	Michael Pyzocha	2137	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 July 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
    closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3, 5-9, 17-20, 25-27, 29 and 30* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 5-9, 17-20, 25-27, and 29-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
    application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-3, 5-9, 17-20, 25-27, and 29-30 are pending.

2.   Amendment filed on 07/22/2005 with a request for continued

examination has been received and considered.

Claim Rejections - 35 USC § 112

3.   The rejections under the second paragraph of 35 U.S.C. 112

have been withdrawn based on the filed amendments.

Claim Objections

4.   The claim objections have been withdrawn based on the filed

amendments.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which

forms the basis for all obviousness rejections set forth in this

Office action:

> (a) A patent may not be obtained though the invention is not identically
> disclosed or described as set forth in section 102 of this title, if the
> differences between the subject matter sought to be patented and the prior
> art are such that the subject matter as a whole would have been obvious at
> the time the invention was made to a person having ordinary skill in the
> art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

6.   Claims 1-3, 5-9, 17-20, 25-27, and 29-30 are rejected under

35 U.S.C. 103(a) as being unpatentable over Matyas, Jr. et al

(US 6687375), further in view of Chen et al (US 6182220),
further in view of Hardy et al (US 6073242), and further in view
of AASAA et al (JP 08037138).

As per claims 1, 17 and 25, Matyas Jr. et al discloses
initializing a pseudo-random number generator (PRNG); obtaining
local seeding information from a host; obtaining additional
seeding information; and stirring the PRNG with the local
seeding information and the additional seeding information (see
column 9 lines 19-34 and 45-67).

Matyas Jr. et al fails to disclose securely obtaining
additional seeding information from one or more remote entropy
servers.

However, Chen et al teaches obtaining seeding information
from one or more remote entropy servers (see column 1 line 66
through column 2 line 9).

At the time of the invention it would have been
obvious to a person of ordinary skill in the art to obtain the
additional seeding information of Matyas Jr. et al from the
server of Chen et al.

Motivation to do so would have been too update passwords on
the server (see Chen et al column 4 lines 15-39).

The modified Matyas Jr. et al and Chen et al system fails to disclose the communication between host and server being secure.

However, Hardy et al teaches secure communications (see column 3 lines 54-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Hardy et al's method of secure communications in the modified system of Matyas Jr. et al and Chen et al system.

Motivation to do so would have been to provide confidentiality, authentication and integrity to the communications (see column 3 lines 54-67).

The modified Matyas Jr. et al, Chen et al and Hardy et al system fails to disclose the securely obtaining seeding information from the one or more remote entropy servers is repeated for redundant entropy servers.

However, AASAA et al teaches the method of repeating a process for redundant servers (see translated abstract).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use AASAA et al's method of obtaining information from two servers in the modified Matyas Jr. et al, Chen et al, and Hardy et al system.

Motivation to do so would have been to compare the

responses from both servers (see AASAA et al abstract).

As per claims 2-3 and 26-27, the modified Matyas Jr. et al,

Chen et al, Hardy et al, and AASAA system discloses the

initializing the PRNG comprises initializing the internal state

of the PRNG with a random value that is a seed (see Matyas Jr.

et al column 9 lines 19-34).

As per claims 5 and 29, the modified Matyas Jr. et al, Chen

et al, Hardy et al, and AASAA system discloses the one or more

remote entropy servers maintain random state pool to supply the

host with the random value (see Matyas Jr. et al column 9 lines

45-67).

As per claim 6-8, the modified Matyas Jr. et al, Chen et

al, Hardy et al, and AASAA system discloses the securely

obtaining seeding information from the one or more remote

entropy servers may include using a privacy protocol, wherein

the privacy protocol comprises secure sockets layer (SSL)

protocol and transport layer security (TLS) protocol (see Hardy

et al column 3 lines 54-67).

As per claims 9 and 30, the modified Matyas Jr. et al, Chen

et al, Hardy et al, and AASAA system discloses the stirring the

PRNG comprises producing a cryptographically random stream of

bits (see Matyas Jr. et al column 9 lines 45-67).

As per claim 18, the modified Matyas Jr. et al, Chen et al,
Hardy et al, and AASAA system discloses the local system
generates local seeding information (see Matyas Jr. et al column
9 lines 45-67).

As per claim 19, the modified Matyas Jr. et al, Chen et al,
Hardy et al, and AASAA system discloses the one or more remote
systems generate remote seeding information (see Chen et al
column 1 line 66 through column 2 line 9).

As per claim 20, the modified Matyas Jr. et al, Chen et al,
Hardy et al, and AASAA system the entropy servers are hardware
or software (see Chen et al column 4 lines 40-54).

Response to Arguments

Applicant's arguments filed 07/22/2005 have been fully
considered but they are not persuasive. Applicant argues: the
system of AASAA is not the same as securely obtaining seeding
information from the one or more remote entropy servers, which
is repeated for redundant entropy servers; and the server in
AASAA is a back-up server and not an entropy server.

Regarding Applicant's argument that the system of AASAA is
not the same as securely obtaining seeding information from the
one or more remote entropy servers, which is repeated for
redundant entropy servers, AASAA is relied upon for its teaching

of repeating the step of obtaining information for back-up

(redundant) servers. When this method is applied to the

modified Matyas Jr. et al, Chen et al, and Hardy et al system

the servers of AASAA are remote entropy servers which seeding

information is securely obtained.

Regarding Applicant's argument that the server in AASAA is

a back-up server and not an entropy server, alone the server in

the AASAA reference is not an entropy server, however, when

modified for the modified Matyas Jr. et al, Chen et al, and

Hardy et al system the servers of AASAA are entropy servers.

Conclusion

7.   The prior art made of record and not relied upon is

considered pertinent to applicant's disclosure. IBM Technical

Disclosure teaches repeating a process for redundant servers.

Any inquiry concerning this communication or earlier

communications from the examiner should be directed to Michael

Pyzocha whose telephone number is (571) 272-3875. The examiner

can normally be reached on 7:00am - 4:30pm first Fridays of the

bi-week off.

If attempts to reach the examiner by telephone are

unsuccessful, the examiner's supervisor, Emmanuel Moise can be

reached on (571) 272-3865. The fax phone number for the

organization where this application or proceeding is assigned is
703-872-9306.

Information regarding the status of an application may be
obtained from the Patent Application Information Retrieval
(PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status
information for unpublished applications is available through
Private PAIR only. For more information about the PAIR system,
see http://pair-direct.uspto.gov. Should you have questions on
access to the Private PAIR system, contact the Electronic
Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER